

CreateUrlCacheEntry

Return value buffer must be large enough to store returned path

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-03-21

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 5019 bytes

Attack Category	<ul style="list-style-type: none">• Malicious Input• Path spoofing or confusion problem		
Vulnerability Category	<ul style="list-style-type: none">• Buffer Overflow• Indeterminate File/Path• Unconditional		
Software Context	<ul style="list-style-type: none">• Internet• Filename Management• File Path Management		
Location	<ul style="list-style-type: none">• wininet.h		
Description	<p>Creates a local file name for saving the cache entry based on the specified URL and the file extension. After CreateUrlCacheEntry is called, the application can write directly into the file in local storage. When the file is completely received, the caller should call CommitUrlCacheEntry to commit the entry in the cache.</p> <p>The buffer should be large enough to store the path of the created file (at least MAX_PATH + 1 characters in length).</p>		
APIs	Function Name		Comments
	CreateURLCacheEntry		
	CreateURLCacheEntryA		
	CreateURLCacheEntryW		
Method of Attack	Buffer Overflow attack.		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Generally applicable (limited scope of usage of this API/rule)	The "solution" for a potential buffer overflow is, in essence, one of	Effective.

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

	<p>inspection. The developer needs to ensure that the constructed file name, based on the URL name, will be handled by the buffer pointer returned in the API call.</p> <p>That is, to be safe ensure that lpszFileName is MAX_PATH +1.</p>
Signature Details	BOOL CreateUrlCacheEntry(LPCTSTR lpszUrlName, DWORD dwExpectedFileSize, LPCTSTR pszFileExtension, LPTSTR lpszFileName, DWORD dwReserved);
Examples of Incorrect Code	<pre>/* Improper sizing of file name buffer: * urlname, expected_file_size, file_extension are all defined previously */ LPTSTR file_name [20]; //What happens if the path is longer than 20? Buffer Overflow bool ret = CreateUrlCacheEntry(url_name, expected_file_size, file_extension, file_name, 0)</pre>
Examples of Corrected Code	<pre>/* Proper sizing of file name buffer: * urlname, expected_file_size, file_extension are all defined previously */ LPTSTR file_name [MAX_PATH + 1]; //The buffer will be long enough for any path the OS could return. if (! CreateUrlCacheEntry(url_name, expected_file_size, file_extension, file_name, 0)) return false;</pre>
Source References	<ul style="list-style-type: none"> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wcesdkr/html/_wcesdk_createurlcacheentry.asp²

	<ul style="list-style-type: none"> • http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wininet/wininet/createurlcacheentry.asp³ • Mustafa, Boulent. Embedded Visual C++, Wininet and htaccess authentication⁴ (2004). 	
Recommended Resource		
Discriminant Set	Operating System	<ul style="list-style-type: none"> • Windows
	Languages	<ul style="list-style-type: none"> • C • C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>